# Planning Taiwan Access Management Federation (TAMF) based on Shibboleth

Naicheng Chang[1], Limei Chen [2], Alan Hopkinson [3]
[1]General Education Center, Tatung University, Taiwan
ncchang@ttu.edu.tw
[2] Library of the Institute of Earth Sciences, Academia Sinica, Taiwan
april@earth.sinica.edu.tw
[3] Learning Resources, Middlesex University, United Kingdom
a.hopkinson@mdx.ac.uk

**Abstract** There are a number of different ways in which it may be verified that a user at a computer attached to the internet may be certified as being entitled to use an electronic resource (usually one that has to be paid for) held on a server elsewhere on the internet. Authentication by Internet Protocol is appropriate when the user is in a fixed environment but to enable a user to have wider access other mechanisms are needed, the most universally applicable being authentication relying on the information provided by an access management federation using Shibboleth. Shibboleth is a standard-based, open source software package for web single sign-on across or within organizational boundaries. It allows sites to make informed authorization decisions for individual access of protected online resources in a privacy-preserving manner. The requirements for the security of the solution particularly regarding the intellectual property rights of the owners of the data are discussed. Various possible solutions are outlined based on those in use in the UK Federation, the US InCommon system, the Swiss SWITCHaai, and the Australian Access Federation. The framework and development leading to the implementation of the Taiwan Access Management Federation (TAMF) primarily follow the SWITCHaai and to a lesser extent the other three Federations. The history, management structure, software used and the organization participants in the four federations that TAMF follows are discussed. The progress of TMAF is described as well. It is hoped that this could serve as a model for federations around the world.

**Keywords:** Taiwan Access Management Federation (TAMF); Access Management; Shibboleth; Security Assertion Markup Language (SAML); Authentication and Authorisation Infrastructure (AAI)

## 1. Issues of Cross-organizational Access Management

Cross-organizational access management results in crucial problems when considering licensing agreements for networked information resources among institutions. It is universally known that there is no demonstrable solution for access management to the many heterogeneous electronic resources that academic and university libraries provide for users, such as the full texts of electronic journals and books, electronic databases, among many others. At present, there are four methods commonly used to access electronic resources among organizations. The first uses an IP address restriction: this method has its advantages; however, the restriction cannot meet the increasing need for off-campus access by users. Second, an IP address restriction using proxy-servers is available whereby with the help of an intermediate server, proxy-servers offer a virtual connection between the user and an IP-restricted resource but this is unfortunately technically challenging for users. Third, a Virtual Private Network (VPN) method which has yet to be fully evaluated is now gradually replacing proxy-servers. Finally, there is individual registration of individual users to take advantage of individual resources. In addition, some otherwise unnoted privacy concerns arise as some users may not be willing to reveal their identities to a resource

provider (i.e. service provider (SP)) if the use of the material is commercially or politically sensitive. More typically, exchanges of personal data between the identity provider (IdP) (i.e. institution) and a resource provider open opportunities for identity deception or theft (Garibyan 2007).

Lynch (1998) addressed seven crucial elements when considering a viable solution to a robust access management. **Feasibility and deployability** points out there should be a simple and standard-based interface such as a web browser between resource providers and identity providers. **Authentication strength** implies both resource providers and identity providers are confident in credentials with the access management infrastructure. **Granularity and extensibility** means resource providers are able to limit access to a resource to a specific closed user community, thus granular access management is likely to be complex due to various policies from institutions. **Cross-protocol flexibility** specifies a highly robust cross-protocol technology and standards are needed to meet this end. **Privacy considerations** mean recognising the need for a secure environment; it is important that all parties to the authentication and authorisation infrastructure should support privacy in the licensing of networked information resources. **Accountability** suggests all parties recognise that the resource being licensed is of value and that the rights of the licensor must be respected. **Ability to collect management data** points out the conflict between gathering management data and privacy which may be resolved mostly at the institutional policy level.

## 2. Shibboleth Solution

Both the U.S. and the U.K. have been actively developing Shibboleth as a solution for access management to restricted electronic resources since 2000 (Internet2) (2008) (JISC: Shibboleth) (2009). Shibboleth, an open source software under the development of Internet2/MACE (Middleware Architecture Committee for Education), has become an emerging global standard for access management to restricted electronic resources.

The aims of Shibboleth are to improve the way in which users access resources throughout the educational and research sectors. Specifically, the goal is to allow users to access internal and external resources seamlessly using a single, institutionally controlled identity. This will substantially reduce current problems in which users are restricted in some IP ranges or are required to maintain multiple passwords for multiple resources in multiple domains. Major benefits of Shibboleth include: (1) reducing the time needed to manage and access protected resources such as sharing resources among several institutions and managing a large number of accounts; (2) increased security (Single SignOn - SSO – removes the need to remember multiple passwords, acquire information about the users from reliable providers, etc.); and (3) interoperability with similar standard-based solutions. Shibboleth is based on Security Assertion Markup Language (SAML) and is thus compatible with other SAML-based software (JISC: UK) (2010).

Using Shibboleth, the benefits for the users include: (1) needing to sign on only once to various protected resources; (2) no IP restriction for access; (3) no need to remember different usernames and passwords; (4) privacy protection because only the users' attributes are released from the identity providers to the service providers, who only roughly know where the user is from; and (5) the same methodology of access to resources from inside or outside the subscribing institution's network, particularly useful for multi-site institutions without a homogenous network. The advantages for the institution are: (1) a cost reduction in password support; (2) the scale of the users is under control; and (3) different categories of users are able to access different levels of resources.

The Shibboleth system provides a standardized mechanism in identity management, and requires strict personal data protection and privacy which is very different from the other alternatives. Thus, it can be seen that most federated access management systems are based on Shibboleth technology as it has been the most widely used technology in education and government which require high level identity management and data privacy. We will discuss this further in the following paragraph. Shibboleth is enterprise- and federation-oriented and has good community support in functionality. However, very few federations have adopted different solutions: the Norwegian Federation was originally based on Sun Access Manager as they found Shibboleth in its earlier versions lacking in functionality (citation). More recently, the Norwegian Federation has been subsumed within a pan-Nordic System, the Kalmar Union (2010), which is using the latest SAML2.0 technology which is the same technology used by the latest version of Shibboleth. More interoperability models of federations will be discussed in Paragraph 4. There are alternative AAI systems available but usually only within one country. In Spain, the national network RedIRIS has developed PAPI (Shibboleth compatible) as an alternative AAI to Shibboleth (citation). In the Netherlands, SurfNET has developed open source A-Select which is non-standard (citation). It is the trend that each AAI system team is actively working in ensuring the interoperability of the AAI elements with other components, in order to make possible global-scale distributed AA infrastructures. Furthermore, when comparing the websites of PAPI, A-Select, and Shibboleth, PAPI has updated its information to 2009, A-Select to 2007; whereas, Shibboleth has updated its website to 2010 with on-going activities described there.

## 3. Background and features of the four federations: UK Federation (UKF), US InCommon (InCommon), Swiss SWITCHaai (SWITCHaai) and Australian Access Federation (AAF)

The U.K. was the first country to initiate a simple and single sign-on solution in 1994 known as “Athens” supported by the Joint Information Systems Committee (JISC) for the access of multiple restricted online resources. The UK Federation (UKF) (2010) was launched in November 2006 and has been operated by JISC and Becta (*British Educational Communications and Technology Agency*) in developing and implementing next generation access management systems based on Shibboleth technology, on behalf of the UK education and research community.

InCommon Federation (in US) (2010), starting its running in 2004, is to create and support a common framework for trustworthy shared management of access to on-line resources in support of education and research in the United States.

SWITCHaai (in Switzerland) (2010) started to run in August 2005 by SWITCH, a non-profit organization providing backbone and develops innovative and unique internet services for the Swiss universities. Originally, SWITCHaai was focused on serving e-learning for college students in Switzerland; however, now the services have been extended to e-journals, research databases, student administration and web mail among others.

A testbed federation named Meta Access Management System (MAMS) ran by Macquarie University in Sydney was decommissioned in November 2009 and migrated to Australian Access Federation (AAF) (2010). The aim of the AAF is to provide a means of allowing a member institution to trust the information it receives from another member to support effective

collaboration between users. AAF is managed by an interim Executive Committee consisting of members from the Council of Australian University Directors of Information Technology and various stakeholders. AAF is the newest federation among the four, and now is actively seeking for international resources sharing with other international federations.

The Table 1, 2 and 3 in the paragraph below provide an overview of the characteristics of each federation. Table 1 covers aspect in federation organization and status including the federation organization structure, participants, funding, and status. Table 2 covers aspects of federation policy and management including federation prominent service, data protection, and federation privacy. Table 3 covers aspects of federation technology and software protocols including protocols, federation schema, and certificate acceptance.

Table 1: Federation organization and status

(organisation structure; participants; funding; status)

| InCommon | UK Federation | SWITCHaai | AAF |
|---|---|---|---|
| Limited Liability Company (LLC); 1.Steering Committee 2.Technical Advisory Committee 1.higher education 2.government and non-profit laboratories 3.research centres 4.agencies 1. federation members 2. sponsored partners more than 240 federation members and sponsors and 4.5 millions end users | JISC; 1. Advisory Board 2. Technical Advisory Group 1.higher education 2.research centres 3.extention education 4.schools 1.JISC and Becta more than 800 federation members and 3 millions end users | SWITCH; 1. Advisory Committee 2. Operations Committee 1.higher education 2.research centres 1.SWITCH 2.federation members more than 80 federation members and 0.27 millions end users | The AAF Incorporated; 1. Executive Committee 1.higher education 2.government participants 3.research centres 4.agencies 1.government 2.federation members more than 60 federation members and 0.24 millions end users |

UKF and SWITCHaai are supervised by their higher education units, JISC in the UK and SWITCH in Switzerland; whereas, InCommon and AAF are governed by a commercial Limited Liability Company (LLC) and AAF Incorporated respectively. The four federations set up committees or advisory boards to operate their management. For example, InCommon has a Steering Committee responsible for managing the business of InCommon and Technical Advisory

Committee relating to the operation and management of InCommon; SWITCHaai has an Advisory Committee helping to set up policies and framework and representing the interests of the federation members and Operations Committee discussing the technical aspects for the federation.

Besides adopting the same Shibboleth technology, the four federations have from the beginning mainly served higher education and research institutions as their central focus. From Table 1, we can see that apart from InCommon and AAF which include government agencies, members of the four federations come mainly from higher education and research institutions. They act as identity providers, and some wear two hats as identity providers and service providers at the same time. As to federation funding, there are three types of funding: (1) federation membership/participants fee: InCommon does not have regular government support, so funding mainly derives from the registration fees and annual fees of their IdPs and SPs, also from the commercial sectors (sponsored partners) such as IBM and Microsoft to support the further development of Shibboleth; (2) government support: JISC and Becta support UKF is the case, though in fact this is supplemented by revenue from membership; and (3) support both from federation members and government: SWITCHaai and AAF are such cases.

InCommon has the most versatile federation members of the four, which includes commercial sponsor partners (that is SPs), and also it started the earliest among the four; therefore, it has the largest amount of end users.

Table 2: Federation policy and management

(prominent services; personal data protection and privacy)

| InCommon | UK Federation | SWITCHaai | AAF |
|---|---|---|---|
| 1.e-research<br>2. metadata management<br>3. web application services<br>4. building communities and others | 1. e-journal<br>2. database and e-learning resources<br>3.video conference and others | 1. e-learning resources<br>2. scientific computing<br>3. e-research and others | 1. e-research<br>2. e-learning resources and object collections<br>3. research infrastructures and others |
| 1.InCommon Federation: Participant Operational Practices | 1.Federation Rules of Membership<br>2.Recommendations for Use of Personal data | 1.AAI Service Agreement | 1.Austtralian Privacy Act 1988 |

For the federation services, at the beginning, UKF was focused on serving library electronic journals and databases, SWITCHaai was mainly on e-learning for college students and InCommon serves web application services. Nevertheless, federation services are now widely applied for resources like scholarly resources and publications, e-learning resources and object collections, scientific instruments, computer facilities, data and other research infrastructures, which

especially can be seen in a newly established federation like AAF.

It is the rationale behind the Shibboleth AA infrastructure that it regulates federation participants who must respect the legal and organizational privacy constraints on attribute information provided by other participants, and use it only for its intended purposes. Therefore, it is important that federation members must comply with any applicable legislation in relation to data protection and privacy. From Table 2, we see the four federations all have their relative regulations and policies for personal data protection and privacy.

Table 3: Federation techonology and software protocols

(protocols; federation schema; certificate accepted)

| InCommon | UK Federation | SWITCHaai | AAF |
|---|---|---|---|
| 1.SAML | 1.SAML | 1.SAML | 1.SAML |
| 2. LDAP | 2. LDAP | 2. LDAP | 2. LDAP |
| 1.eduPerson | 1.eduPerson | 1.SwissEduPerson | 1.auEduPerson |
| 1.InCommon | 1.JANET Server | 1.self-signed | 1. The AAF |
| Certificate | Certificate | 2. accepted | Incorporated |
| Service | Service (SCS) | Certification | 2. accepted |
| 2.self-signed | 2. accepted | Authority (CA) | Certification |
| 3. accepted | Certification | | Authority (CA) |
| Certification | Authority (CA) | | |
| Authority (CA) | | | |

The four federations all use the most recognized SAML or SAML compatible technology which provide confidentiality and authentication/integrity. Also, the four federations use the Lightweight Directory Access Protocol (LDAP) software to build up their user databases. The latest versions for SAML and Shibboleth are SAML 2.0 and Shibboleth 2.x.

Federation schema is the core of an AAI system. Careful evaluation before building identity access management system is highly required. InCommon and UKF use the eduPerson schema, SWITCHaai has SwissEduPerson, and AAF has auEduPerson. Both SwissEduPerson and auEduPerson are derived from eduPerson schema.

There are three methods to be certified in a Shibboleth system: issued by federations, self-signed, or certified by an accepted Certification Authority (CA) such as UK e-Science Certification Authority Server certificates which acts as issuers for certificates. In either way, by signing a SAML assertion, the certificate enables the recipient to properly identify the sender as well as to verify the assertion's integrity. On the other hand, by using the recipient's certificate to encrypt an assertion, the sender ensures that only the intended recipient can access the assertion's content.

In general, SWITCHaai recommends using a self-signed certificate with a three-year validity. Also, it accepts certificates issued under a well-known CA like Microsoft. AAF accepts certificates issued by AAF or its approved certificate authorities. UKF accepts certificates issued by JANET or from any trusted certification authority. InCommon offers the InCommon Certificate Service to the higher education community, at the same time, InCommon also authorizes commercial CA (such as Comodo CA, Ltd) to issue certificates.

## 4. Planning the Taiwan Access Management Federation (TAMF)

Taiwan is an independent island off the mainland of China with a population of just over 20

millions and an area of 36,000 km$^2$. Politically, it suffers a certain level of isolation but, technically and in the sphere of education, it has links with all the major industrialised countries. Universities purchase all the major electronic resources as could be found in the most advanced economies in the world.

The Taiwan Access Management Federation (TAMF) has been planned based on the success of four production federations: UK Federation (UKF), InCommon, SWITCHaai, Australian Access Federation (AAF), and also based on a prototype of a virtual federation by implementation of Shibboleth in Academia Sinica in Taiwan. Academia Sinica is a prominent research institution with a world-wide reputation. There are 18 libraries supporting research for twenty-four research institutes and seven research centres devoted mainly to three research disciplines: mathematics and physical sciences, life sciences, and the humanities and social sciences.

## The first prototype Shibboleth system in Taiwan

As there is very limited knowledge about Shibboleth in Taiwan, in July 2008, for the first phase the Prototype joined the Meta Access Management System Tested Federation (MAMS) to gain more knowledge regarding the operation of Shibboleth (Macquarie University 2008). An IdP was set up at the Library of the Institute of Earth Sciences, Academia Sinica (ASIES) (2010) to provide user information and authenticate the users as well as requesting Shibboleth-based access services from some participating Shibboleth publishers like Elsevier, ProQuest and Thomson Reuters, Ltd. who are resource providers of the ASIES library. MAMS was decommissioned at the end of November 2009 and part of it migrated to the Australian Access Federation. The second phase of the study then began where the Computing Center of Academia Sinica (ASCC) played the role of issuing and managing certificates for the users. The Chinese Geoscience Union, Taipei, a society with about 250 members and subscribers publishes a SCI journal entitled “Terrestrial, Atmospheric and Oceanic Sciences (TAO)” is also interested in how to go through Shibboleth operation to enforce access control to their resource and users and set up an SP at their site as well. The Shibboleth virtual federation then was formed by implementing the IdP, SP and the ‘Where Are You From (WAYF)” (ASCC) as shown in Figure 1.

The Shibboleth architecture diagram used to delineate the Shibboleth virtual federation was a modification of the original schema provided by the Swiss Education and Research Network (SWITCH) (2010) and the diagram by Klingenstein (Klingenstein 2008) (see Figure 1). In the Figure, there are four components: (1) the user is a research fellow from Academia Sinica, who tries to gain online access to an article available at Science Direct, Elsevier; (2) the libraries of Academia Sinica as an IdP with which the user is registered; (3) The SPs as Elsevier, ProQuest Thomson Reuters, Ltd., CGU which provide restricted resources and have access control systems to decide whether the user should be allowed to access the resources, and if, yes, at what level; and (4) The “Where Are You From” (WAYF) service, a centralized service operated on behalf of the Shibboleth Federation. Here the “WAYF” was MAMS at the first phase of the study and was replaced by the Computing Centre, Academia Sinica.

The stages for the user to complete for his or her access are indicated in the figure. In stages 1 and 2, the user connects to any of the resources and is redirected to the appropriate organization; in the third, fourth and fifth stages, the user makes a selection for his/her home organization and the user authentication at his/her home organization is ascertained; and finally, access to the resource is approved.

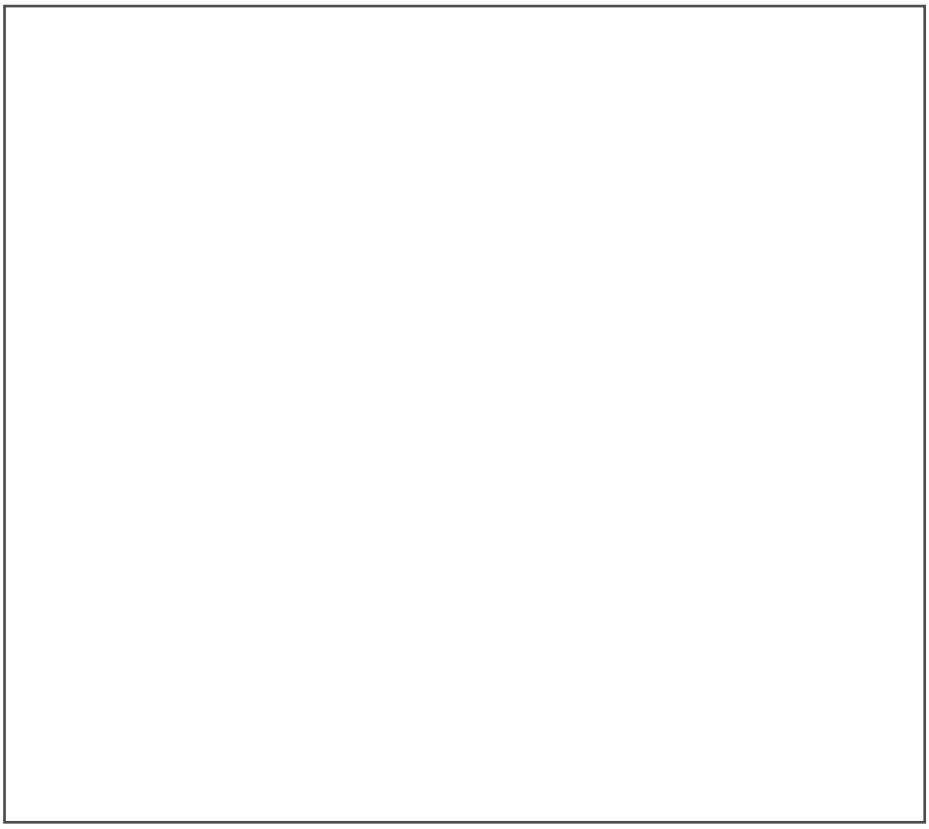

Figure1: Shibboleth architecture diagram used in this pilot project (modified from the diagrams provided by SWITCH and Klingenstein).

Concerning the technology for software installation, as a library representing the IdP, we will mention here only the IdP environment that was set up. Debian GNU/Linux 5.0 version was adopted for the operating system and Shibboleth version 1.3c was installed at IP domain name: idprovider.earth.sinica.edu.tw. A user database was also set up using Lightweight Directory Access Protocol (LDAP) with a total of 150 users from ASIES.

**Taiwan Access Management Federation (TAMF)**

The design of the structure of TAMF is based on SWITCHaai as shown in Figure 2. The reasons we primarily follow the architecture of SWITCHaai are because it has a very solid federation authentication and authorization infrastructure (AAI) clearly depicted and is easy to be adopted while the other three federations are more ambiguous in this aspect. The construction and operation of TAMF that are mostly adopted from the merits of the four federations after comparison will be discussed in three categories: (a) federation organization and status; (b) policy and management; and (c) federation technology and software protocols.

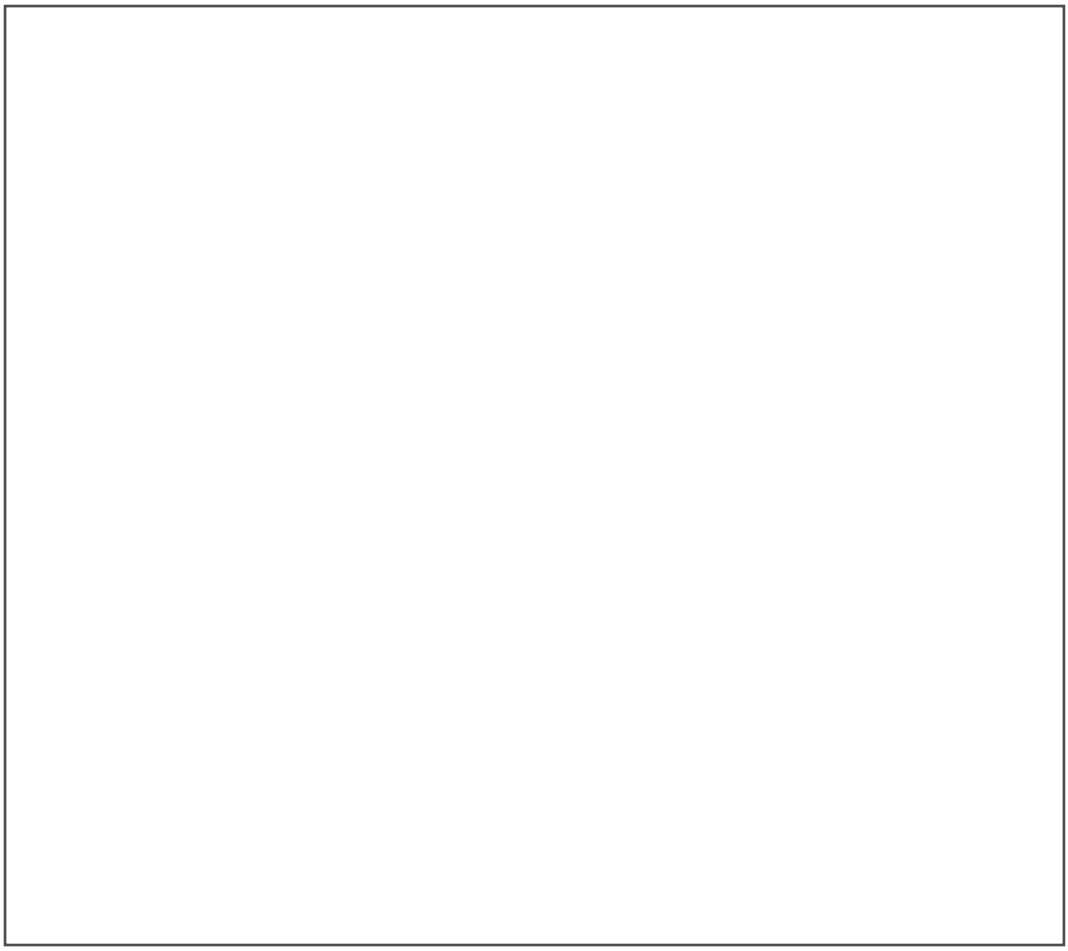

Figure 2: Taiwan Access Management Federation (TAMF)

### A. Federation organization and status

As discussed in Paragraph 3, UKF and SWITCHaai are supervised by their higher education units, JISC in UK and SWITCH in Switzerland; whereas, InCommon and AAF are governed by a commercial Limited Liability Company (LLC) and AAF Incorporated respectively. The National Science Council (NSC) (2010b) would be the ideal driver to establish TAMF and be the lead operator in its management. NSC in Taiwan provides a world-class network and infrastructure, TaiWan Advanced Research & Education Network (TWAREN) (2010), which is running Grid-enabled applications as shown in Figure 3; provide the networking infrastructure for services to access to electronic resources; new environments for learning, teaching, and research.

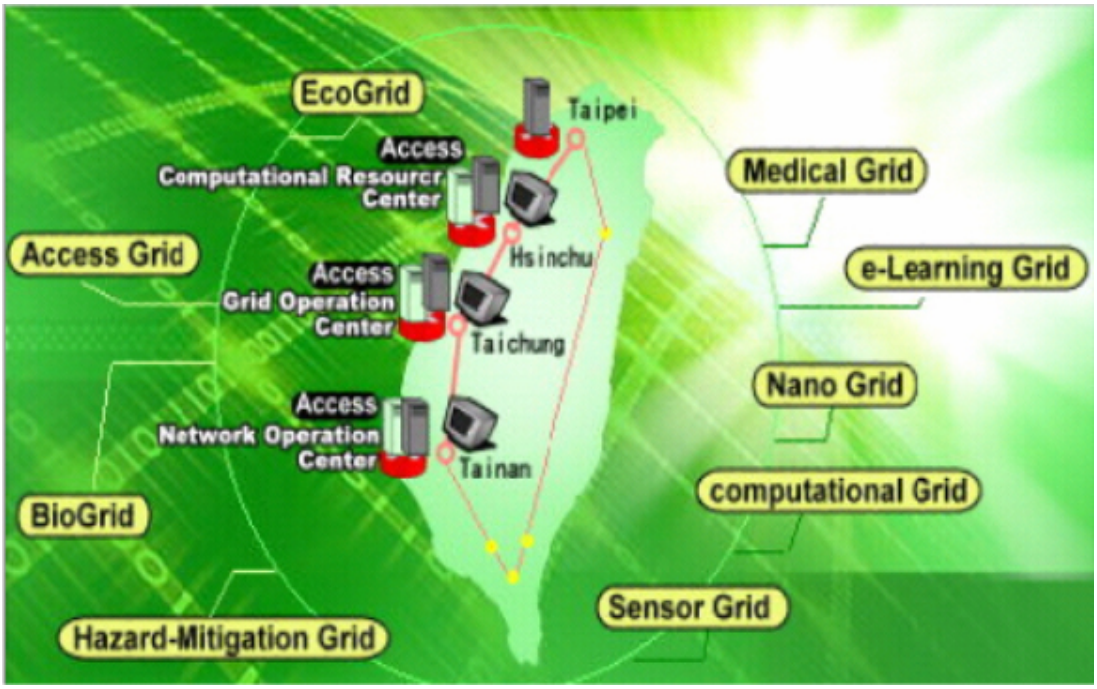


Figure 3: TaiWan Advanced Research & Education Network (TWAREN)

TAMF infrastructure will facilitate trusted electronic communications and collaboration within and between Taiwan and international higher education and research institutions. The mission of the TAMF is to create and support a common framework for trustworthy shared management of access to online resources in support of education and research in Taiwan. TAMF adopts SWITCHaai's structure and will be managed by its Advisory Committee and Operations Committee as shown in Figure 2. The Advisory Committee is responsible for managing the business and affairs of TAMF and its federation, including oversight and recommendations on issues arising from the operation and management of the TAMF Federation. The Operations Committee is responsible for policy implementation, technical operations, identity verification, and support of TAMF and its federation participants.

We discussed in Paragraph 3 that there are three types of funding: federation membership/participants fee, government support, and support both from federation members and government. We suggest that NSC in Taiwan should take full responsibility for building up TAMF and providing full financial support for the operation of TAMF for the initial phase and there will be a registration fee and annual fee later for IdPs but not for SPs. In order to secure benefit for IdPs, SPs can only be federation partners but not federation members.

## B. Policy and management

Grid services have recently become an important area for a national research and education network which aims to introduce to different areas Grid services for scientific research purposes, making use of distributed computing services. TAMF will take advantage of TWAREN and provide resources particularly in e-journals, e-databases, scientific computing, and e-learning

resources from our National Taiwan e-Learning and Digital Archives Program. More federation services can be provided as needed.

A confederation implies an agreement among the various federations; yet, in a federation peer members of different federations can peer among each other. A confederation has several benefits. Certainly, resources and services sharing is one more benefit in that international take-up secures the future of development and support, and also saves money through work in partnership. One notable example of confederation is Kalmar Union discussed in Paragraph 2, which started in 2008, and has been established as a cross-federation of the Nordic academic identity federations. It is a cross-Nordic authentication system for higher education and research among federations in Finland, Norway, Denmark, Sweden, and Iceland. Another well-known confederation is Eduroam (education roaming) (2010) confederation. Eduroam is a networking confederation which provides a secure, world-wide "roaming" access service developed for the international research and education community under which authenticated individuals are able to access the resources to which they have access at their home institution when they are situated in another institution in the confederation.

InCommon is considering cooperating with UKF; UKF has been proposing inter-federation with the UK Government Gateway; `SWITCHaai is joining eduGAIN` which will enable the sharing of identity data between federations. AAF will engage with the international Federation community through the Research and Education Federations (REFeds) group coordinated by TERENA (citation). REFeds includes representatives from 23 existing research and education federations from Europe, North America, Asia, Australia and several federations in the process of forming. Engagement with international community is certainly a way that AAF will go. TAMF will propose an international liaison plan initially with China (CARSI-Fed/CERNET-Fed) (2008) and Japan (UPKI) (2010), both of which are based on Shibboleth.

### C. Federation technology and software protocols

SAML standard and Shibboleth technology are two key components in an Authentication and Authorisation Infrastructure (AAI). The two are properly received by most access management federations. Shibboleth technology consists of a set of protocols and mechanisms linking multiple IdPs, SPs and users together. IdP and IdP+SP request subscription service from AAI service, whereas IdP+SP and SP request resource registration from AAI service as shown in Figure 2. SAML is a flexible eXtensible Mark-up Language (XML)-based framework. SAML has gained widespread industry adoption, particularly high potential applications in web single sign-on and securing web services. TAMF will certainly take advantage of this well-received technology and interoperate into global trend. As to federation schema, Both SwissEduPerson and auEduPerson are derived from the eduPerson schema, so TAMF could develop its eduPerson schema based upon the four federations to identify its core attributes, unique identifier and so on.

In order to obtain proper protection from being certified in a Shibboleth system, there are three methods of to be certified in a Shibboleth system: issued by federations, self-signed, or certified by an accepted Certification Authority (CA) which acts as issuers for certificates. TAMF could start with self-signed and certified by an accepted Certification Authority which is the main trend when observing the development of certification policies from InCommon and SWITCHaai.

## 5. Discussion

Taking the examples of the successful federations in Europe, US, and in Australia, TAMF has a good chance to succeed. It is our view that planning for NSC as the driver and operator, TAMF has an excellent chance of survival for the following reasons. Firstly, TWAREN under NSC is a member of eduroam. A TAMF researcher is able to collaborate more easily via eduroam by simply opening his laptop with colleagues in Taiwan and in other countries with which TAMF has a peering relationship. Secondly, the success of CONCERT (CONsortium on Core Electronic Resources in Taiwan) organized under NSC**, which** takes advantage of the growing popularity of web-based full-text documents, does its best to fully exploit the economies of group purchase and resource-sharing (NSC 2010a). NSC has been making good communication with nationwide institutions, users, and resource providers through the operation of CONCERT. Thirdly, NSC launched a five-year National Science & Technology Program of e-Learning with excellent achievements (NSC 2003). TAMF will provide the means to access seamlessly these e-learning resources and learning objects.

Furthermore, issues of data protection and privacy are major themes in access management federation as discussed in Paragraph 3. In Taiwan, the Act of Protection of Personal Data was passed by the Legislative Yuan in April 2010. A safe environment like TAMF to secure communication and support effective collaboration between users is urgently demanded. Increasing the likelihood that TAMF will survive is the fact that TAMF is able to realise the benefits of common access management mechanisms through collaborating well with the nationwide Grid community via TAWREN as addressed in paragraph 3. Lastly, TAMF will certainly go for confederation or building peering relationships with neighbouring federations such as CARSI-Fed/CERNET-Fed in China and UPKI in Japan. It is likely that TAMF will continue to initiate a confederation to connect countries in the Asia Pacific area. This will be called Asia Pacific Shibboleth COlaboration (APSCO). This will help to establish a global-scale confederation.

Given the differences in national law and licensing preferences, expect there to be harsh challenges and potential risks. Davies and Shreeve (2007) pointed out two possible challenges to a common global infrastructure, technical and policy-related. In order to build up a common global infrastructure, technically, a common language is required to communicate among federations. SAML is the one that currently has been globally accepted. There are more challenges such as the management of metadata. If one looks at the policy issues of inter-federation interoperability, the challenges are much more difficult than the technical aspects. Taking the example of the preparation of agreements between federations for the establishment of confederations, this involves setting up rules about joining for IdPs and SPs; the obligations of the federation operator; the mechanisms and practices for data protection and so on. And to achieve the level of successful interoperability, very possibly it has to cross numerous legislative barriers from different nations. In short, this involves issues of whether federation members from the confederation are willing to adhere to rules to establish a trust relationship. Tveter, Melve and Linden (2007) also pointed out that the establishment of trust is an issue far more challenging than the technological ones when outlining considerations for trust management to interconnect the Nordic identity federations.

## 6. Conclusion

It is likely that there will be a significant adoption of TAMF by Taiwan's higher education and research institutions. TAMF is likely to be asked to enable federated access to key service bodies such as e-Government to liaise with government-centric identity initiatives, and also to support the national programme in life-long learning initiatives. TAMF should at the same time look for a sustainable cost model such as members funding the operational costs of TAMF, particularly once a certain level of membership has been achieved.

The SAML standard and Shibboleth technology are currently being widely adopted, and have high potential to be interoperated with web services in the future. Examples currently seen are Shibboleth having interoperability with Microsoft CardSpace and with Google Scholar.

It is understood that the major driver for adoption of federated access management by institutions are increasing national and international inter-institutional collaborations for e-research and e-learning, and to rationalise resources, therefore, confederation is a global trend. At present, many institutions like Academia Sinica in Taiwan have dozens of self-established and valuable databases, yet these databases are distributed among different research institutes and centres that do not have a proper access management protocol. It is likely that this prototype in Academia Sinica will be adopted by the authorities. Although there may be long-term challenges ahead, geographic international federations like APSCO are likely to be the future model for Shibboleth development for institutions in the Asia/Pacific area.

The international federated access management community is more active in Europe than in the Asia Pacific region where China's CARSI-Fed/CERNET-Fed and Japan's UPKI are still at the pilot stage and TAMF as we have seen is in the planning stage. Taking into account the experience of the SWITCHaai federation which spent 4 years from pilot to an operational federation and the UKF which needed 2 years to reach the stage of a working federation, this national federation needs to be set up as early as possible because the environment for building an access management system in Taiwan is mature. TAMF should participate in the international forums related to federation coordination, particularly in academic and research sectors, leveraging TAMF into the international federated access management community.

## References


ASIES. 2010. *Institute of Earth Sciences, Academia Sinica*. URL: http://www.earth.sinica.edu.tw/en/ [viewed January 12, 2010]

Australian Access Federation. 2010. *Australian Access Federation: providing trustedaccess to services, resources and people*. URL: http://www.aaf.edu.au[viewed January 12, 2010]

CARSI-Fed/CERNET-Fed. 2008. URL: http://carsi.edu.cn/index.jsp [viewed January 12, 2010]

Davies, C. and M. Shreeve. 2007. *Federated access management: international Aspects*. Guildford: Curtis+Cartwright Consulting Ltd..

Eduroam. 2010. ***E****ducation roaming.* URL: http://www.eduroam.org [viewed January 12, 2010]

Garibyan, M. 2007. *Building a national federated access management infrastructure : the U.K. experience*. Paper presented at the ITE 2007 Conference in Yerevan.

InCommon. 2010. *InCommon makes sharing protected online resources easier.* URL: http://www.incommonfederation.org [viewed January 8, 2010]

Internet2. 2008. *Shibboleth: a project of the Internet2 middleware initiative*. URL: http://shibboleth.internet2.edu [viewed July 5, 2008]

JISC. 2008. *U.K. federated access management*. URL: http://www.jisc.ac.uk/federation [viewed January 16, 2010]

JISC. 2009. *Shibboleth: connecting people & resources briefing (version 2)*. URL: http://www.jisc.ac.uk/publications/publications/pub_shibboleth.aspx [viewed December 20, 2009]

Kalmar Union. 2010. URL: http://www.kalmar2.org/kalmar2web/front_page.html [viewed December 2, 2009]

Klingenstein, N. 2008. *Shibboleth 2.0: finally.* Paper presented at Trans-European Research and Education Networking Association, TNC 2008 at Bruges, Belgium. URL: http://tnc2008.terena.org/core/getfile.php?file_id=401 [viewed June 15, 2008]

Lynch, C. 1998. *A white paper on authentication and access management issues in cross-organizational use of networked information resources*. Coalition for Networked Information. URL: http://www.cni.org/projects/authentication/authentication-wp.html [viewed June 20, 2008]

Macquarie University - Sydney. 2008. *MAMS: Meta Access Management System: testbed federation*. URL: http://www.federation.org.au/FedManager/jsp/index.jsp [viewed June 29, 2008]

NSC. (2003). *National Science & Technology Program of e-Learning***.** URL: http://elearning.tca.org.tw/index.html [viewed January 12, 2010]

NSC. (2010a). ***Consortium on Core Electronic Resources in Taiwan (CONCERT).*** URL: http://www.stpi.org.tw/fdb/index.html [viewed January 12, 2010]

NSC. (2010b). *National Science Council*. URL: http://web1.nsc.gov.tw/mp.aspx?mp=7 [viewed January 12, 2010]

SWITCH. 2010. *SWITCH: Serving Swiss Universities*. URL: http://www.switch.ch/aai/index.html [viewed December 20, 2009]

Tveter, W., I. Melve, and M. Linden. 2007. Towards interconnecting the Nordic identity federations. *Campus-Wide Information Systems* 24(2): 252–259.

TWAREN. 2010. *TaiWan Advanced Research & Education Network.* URL: http://www.twaren.net/english/ [viewed January 12, 2010]

UK Access Management Federation. 2010. *UK access management federation for education and research*. URL: http://www.ukfederation.org.uk [viewed June 29, 2008]

UPKI. 2010. *University Public Key Infrastructure Initiative*. URL: https://upki-portal.nii.ac.jp/docs/fed/participants [viewed January 12, 2010]

PAPI (shibboleth compatible): http://papi.rediris.es/
A-select 2002-2007 http://a-select.surfnet.nl/home.html
shibboleth http://shibboleth.internet2.edu/
REFEDs: Research and Education Federations http://www.terena.org/activities/refeds/

**Acknowledgement**

Financial support for this research from the National Science Council, Taiwan, under the grant NSC 96-2413-H-036-001 is gratefully acknowledged.